

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
7 February 2002 (07.02.2002)

PCT

(10) International Publication Number
WO 02/11395 A2

(51) International Patent Classification⁷: **H04L 29/00**
(21) International Application Number: PCT/US01/24153
(22) International Filing Date: 31 July 2001 (31.07.2001)
(25) Filing Language: English
(26) Publication Language: English
(30) Priority Data:
09/630,031 31 July 2000 (31.07.2000) US
(71) Applicant (for all designated States except US): **NOKIA NETWORKS OY** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

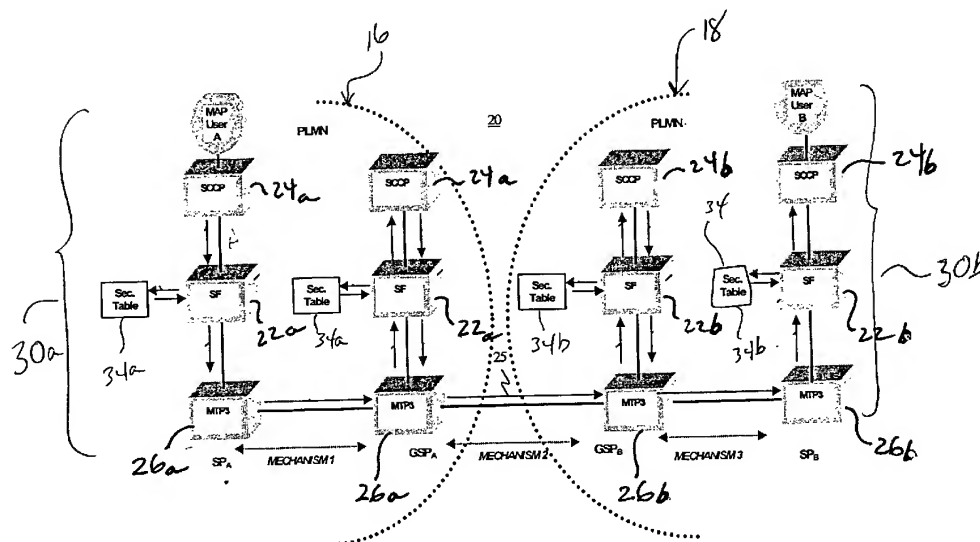
Published:

— without international search report and to be republished upon receipt of that report

(72) Inventor; and
(75) Inventor/Applicant (for US only): **FACCIN, Stefano** [IT/US]; 3421 Dartmoore Drive, Dallas, TX 75229 (US).
(74) Agents: **RIVERS, Brian, T.** et al.; Nokia Inc., 6000 Connection Drive, MS 1-4-755, Irving, TX 75039 (US).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD FOR SECURING INFORMATION EXCHANGES IN A TELECOMMUNICATION NETWORK



(57) Abstract: A system (Fig. 2) and a method are provided for securing signaling connections in telecommunication networks and to provide network functionalities (22a, 22b) to secure the signaling connection between network elements. The security parameters (34) are associated with the addressing of signaling information preferably using global titles (GT) or signaling point codes (SPC). The method for securing signaling connection within communication networks includes the steps of obtaining a security parameter (34) of a second network, using the security parameter (34) to transform the signaling information into a secured signaling information, sending the secured signaling information to the second network entity (26b), and recovering the signaling information from the secured signaling information.



WO 02/11395 A2

METHOD FOR SECURING INFORMATION EXCHANGES IN A TELECOMMUNICATION NETWORK

5 Field of the Invention

The invention relates to telecommunication systems and, more specifically, to security of information exchanged between network elements in the telecommunication network.

Background

10 The signaling network can be seen as the spine of a telecommunication network, both in the fixed and the mobile case. The functions of signaling are to set up a call, to supervise a call, and to clear a call. In particular, mobile telecommunication networks entrust to the signaling network the delivery of information vital for both the service provision, which includes subscriber
15 information, service parameters, and authentication information, and the management of user mobility. If Internet Protocol (IP) is used to transmit SS7 messages, then the open transport architecture of IP will mean that message packets are open to easier manipulation at nodes.

Different signaling standards were developed in different parts of the
20 world. Thus, when a call originates in one network with one type of signaling implementation and terminates in another network with a different type of signaling system, some adaptations are needed. The International Telecommunication Union (ITU) adopted a common system known as the Signaling System Number 7 (SS7). One of the main advantages of this system
25 was that signaling did not have to go along the same path as the speech. SS7 consists of two parts: the Message Transfer Part (MTP), which is responsible for transferring messages; and the Telephone User Part (TUP).

The MTP consists of three sublayers: the lowest level, MTP layer 1, defines the physical and electric characteristics; MTP layer 2, which is for data
30 link control, helps in error free transmission of the signaling messages between

adjacent elements; MTP layer 3, or the network layer, is responsible for taking the message from any element in a signaling network to any other element within the same network.

5 The TUP is the user who receives, sends, and acts on the message. The ITU allowed for small variations in messages within one country alone. These variations in messages are called the National User Part (NUP) and are similar to the TUP.

10 With the introduction of the Integrated Services Digital Network (ISDN), which has a broader capability than Public Switched Telephone Network (PSTN), some extra set of messages were required; these are known as the ISDN User Part (ISUP). Whether it is TUP, NUP, or ISUP they all are performing the same function in helping to set up a call.

15 The combination TUP/MTP alone was not sufficient when virtual connections became necessary. MTP guarantees the transfer of messages from any signaling point in the signaling network to any other signaling point, safely and reliably. However, each message can reach the destination signaling point by using different paths. This may cause situations where the order of messages that are received, are different from the original sequence. Thus, order is important, and also there is a need to establish a virtual connection. Virtual
20 connections use an oriented connection protocol that will provide sequence numbers to enable the messages to be placed in the correct order.

Another instance of when the TUP/MTP structure is inefficient, is when a signaling message has to be sent across multiple networks in the absence of a determined route for a call. MTP is capable of routing a message within one
25 network only. The case of setting up a call across multiple networks is not the same as signaling across the same network. The signaling goes leg by leg according to the call. But in the absence of a determined route for the call, MTP cannot route a signaling message across multiple networks. To solve these problems a Signaling Connection and Control Part (SCCP) protocol layer was
30 created on top of the MTP. The SCCP takes care of virtual connections and connectionless signaling. The tasks of TUP and SCCP are different, and thus, they are parallel to each other, but both use the services of MTP.

In GSM networks, signaling is not as simple as in the PSTN. There are extra signaling requirements due to the different architecture of the network, which requires a large amount of non-call related signaling unlike the PSTN telephone. The subscriber is mobile. Therefore, a continuous tracking of the mobile station is required resulting in what is known as the location update procedure. This procedure is an example of non-call related signaling, where the mobile phone and the network are communicating, but no call is taking place. This requires additional sets of standard messages to fulfil the signaling requirements of GSM networks. These additional protocol layers are: Base Station Subsystem Application Part (BSSAP); Mobile Application Part (MAP); and Transaction Capabilities Application Part (TCAP)

The first of these additional protocol layers, which are specific to GSM networks, is the BSSAP. This layer is used when a Mobile Services Switching Centre (MSSC) communicates with a Base Station Controller (BSC) and the mobile station. Since the mobile station and the MSSC have to communicate via the BSC, there must be a virtual connection therebetween, and, hence, the service of SCCP is also needed. The authentication verification procedure and assigning a New Temporal Mobile Subscriber Identity (TMSI) all take place with the standard set of messages of BSSAP. Communication between MSSC and BSC also uses the BSSAP protocol layer. Therefore, BSSAP serves two purposes: MSSC-BSC signaling and MSSC-Mobile Station signaling.

The example of location update procedure mentioned is not limited to the MSSC-BSC section but spans multiple PLMNs. In case of a first time location update by an international roaming subscriber, the Visitor Location Register (VLR) has to get the data from the subscriber Home Location Register (HLR) via the gateway MSSC of the subscriber's home network.

While a mobile terminated call is being handled, the MSRN has to be requested from the HLR without routing the call to the HLR. Therefore, for these cases, another protocol layer is added to the SS7 called Mobile Application Part (MAP). MAP is used for signaling communication between NSS elements.

In MAP signaling, one MSSC sends a message to the HLR, and that message invokes a certain result. The HLR sends the result back, which may be

the final result or some other messages might also follow. The invocations and results that are sent back and forth between multiple elements using MAP need some sort of secretary to manage the transactions. This secretary is called the Transaction Capabilities Application Part (TCAP).

5 Topologically, the SS7 consists of Signaling Points (SPs) and Signaling Transfer Points (STPs) connected into a distributed network by data transmission circuits known as signaling links. The SPs are nodes in which signaling messages originate and terminate. The STPs are packet switches that provide message routing between adjacent SPs or STPs.

10 All subscribers are issued an IMSI, a unique identity number. A subscriber is always identified within the GSM network by the IMSI. The IMSI can be mapped to a Global Title (GT) to address the subscriber's home Public Plan Mobile Network (PLMN) and HLR. The conversion from an E.212 IMSI to an E.164 Global Title (GT) is given in CCITT (*Comité Consultatif International*
15 *Téléphonique et Télégraphique*) recommendations E.214, the content of which is incorporated herein by reference. The Mobile Country Code (MCC) is converted to a Country Code (CC) and a Mobile Network Code (MNC) to a Network Code (NC). The mapping from one domain to another is a one-to-one and conversion tables can be stored locally. While a Signaling Point Code (SPC) can be used
20 only within a network, GTs allow addressing of any SP globally. The GT can be an E.164 ISDN number identifying the SCCP node and an SSN number identifying the SCCP user. While GSM does not allow the use of an E.212 IMSI to be used as the GT, it can be translated using the procedures defined in E.214 to derive a global title. The GT does not provide routing information, and hence,
25 must be translated to an SPC code. This is done by the SCCP.

 In order to provide authentication of two entities setting-up a dialogue among themselves, together with integrity and confidentiality of data exchanged during the dialogue, a fundamental piece of information is the identity of the involved entities. Although different schemes other than the one described in
30 this invention can be used by the entities to set-up a secure channel without knowledge of the respective identities, this lack of knowledge leads to an

overhead due to the need of respectively assessing and validating the identity of the other entity.

In any of these situations, the first dialogue-initiating MAP entity does not know the real identity of the second peer MAP entity before hand. This happens
5 only when the GT received from the second entity is translated in the SPC of the first entity. Therefore, without any additional mechanism, which is provided by this invention, any security solution introduced at MAP level needs an initial exchange of messages between the two communicating entities just to make both entities aware of their respective identities.

10 As a first example of usage of the GT, the HLR is addressed by the MSSC during a mobile terminated call set-up to discover the whereabouts of the mobile station. The call can be originated either by a mobile subscriber of a different PLMN or by a fixed user, and the MSSC addressing the HLR is a Gateway MSSC in the home network of the called mobile station. The SCCP address is
15 derived from the Mobile Subscriber ISDN (MSISDN) dialled by the calling subscriber, that is translated into either a signaling point code, in the case of communications within the home network, or a global title if the communication is across a network boundary.

As a second example the Visitor Location Register (VLR) might be
20 addressed by another VLR when a mobile station moves from one VLR service area to another. The new VLR can request the subscriber information, such as the authentication triplets from the previous VLR. The new VLR derives the address of the previous VLR from the Location Area Identification provided by the Mobile Station in the location registration request.

25 A peculiar aspect of the GT translation is that, when SCCP receives a Transaction Capabilities Application Part (TCAP) packet and the Called Party Address is a GT, SCCP will translate the GT "to his best knowledge". This means that the translation doesn't necessarily provide the SPC of the recipient as an answer. If the SCCP can't provide the SPC of the recipient, it adds an
30 intermediate SPC that refers to a node that can have knowledge on how the GT should be translated or that can forward the message towards a node that knows

it. The message will then be forwarded towards this intermediate node where the GT will be translated again.

In the PLMN portion of the signaling network two types of nodes exist: internal signaling, which are nodes connected only to nodes that belong to the same network, and Gateway Signaling Points (GSP), i.e. nodes connected to signaling points in other networks.

Generally in cellular networks, each MAP/ANSI-41 node (e.g. VLR, HLR, MSSC, etc.) is a signaling point without GT translation and is connected to two Signaling Transfer Points (STP). STP is instead a signaling point with the SS7 stack up to SCCP and the GT translation function. The term signaling point is referred herein generically to both signaling points and signaling transfer points.

Referring to figure 1, an example of a global translation is given to point out the embedded drawback in the prior art method for carrying out the signaling in the telecommunication networks because the signaling information is only physically secured. Thus, the physical nodes and all the elements of the signaling network are not accessible to unauthorised persons.

When a mobile station, not drawn, registers to a new VLR away from the home network, such as PLMN B, the VLR opens a dialogue with the HLR of the mobile station using the HLR's GT that can be derived from the IMSI, HLR_GT, to reach the HLR. The SCCP in the VLR signaling point will notice that the HLR GT is pointing towards another network. Therefore, the SCCP adds the signaling point code, SPC2, of the gateway STP in PLMN A. The HLR GT is included in the message for subsequent translations.

The SCCP in the gateway STP of PLMN A will translate the HLR_GT into a signaling point code of the gateway STP in PLMN B, SPC3, needed to reach a gateway STP in PLMN B (the SPCs of gateway STP are public in order to allow interconnection of PLMNs).

The SCCP in the gateway STP of PLMN B will translate the received global HLR_GT title into the signaling point code, SPC4, of the STP where the HLR is located. Note that this is the first SCCP node that has knowledge of the real location, which is the SPC of the HLR. The message is sent to the HLR

signaling point where the SCCP layer recognise it as a message for the HLR and delivers it to the HLR.

5 The type of routing shown in the example can be used also for intra-PLMN signaling. When considering large PLMN, i.e. PLMN with a large number of signaling nodes, there may not be a direct link from every node to every other node, as determined by the operator. In this case, the GT translation can be performed step-by-step.

10 As telecommunication networks expand, more and more signaling elements of a signaling network are placed in locations where the risk of an unauthorised entry becomes unacceptably high. Moreover, in telecommunication networks the IP-based signaling architectures are more open than the current signaling networks. The risk that unauthorized parties could monitor the signaling information is unacceptably high. Therefore, what is needed is a system and method for providing a higher level of security in telecommunication networks.

15 Summary of the Invention

A system and a method are provided for securing signaling connections in telecommunication networks and to provide network functionalities to secure the signaling connection between network elements. This is accomplished by sending the signaling information from a first network entity to a second network entity via a secured transferring means. The first network entity has access to the security parameters of the second network entity and the first network entity uses the security parameters to secure the signaling connection between the first network entity and the second network entity. In particular, the security parameters are associated with the addressing of signaling information, preferably using global titles (GT) or signaling point codes (SPC).

25 One advantage is that long-term security associations are established between signaling points, so that "on-line" exchanges and agreement of security parameters are avoided. These long term security associations might be established either by letting every signaling point know the security parameters of every adjacent node-equipped with a security functionality or by adopting, in the network, a centralised security management functionality

Brief Description of the Drawings

Fig. 1 illustrates a global title translation in the prior art.

Fig. 2 illustrates a schematic drawing of PLMN-networks A and B in accordance with the present invention.

5 Fig. 3 illustrates a signaling point of Fig. 1 connected to a security functionality.

Fig. 4 illustrates a Global Title Security Server (GTSS).

Fig. 5 illustrates protocol stacking of a MAP user and GTSS.

Fig. 6 illustrates a signaling node, according to the present invention.

10 Fig. 7 illustrates an Intra-PLMN dialogue using the GTSS of Fig. 4.

Fig. 8 illustrates an Inter-PLMN dialogue using Global Title Security Server of Fig. 4.

Fig. 9 is a flowchart of the process for sending security information between two network entities.

15 Detailed Description

Referring now to figure 2, a schematic drawing of a Public Land Mobile Network (PLMN) network 16 and PLMN network 18 of a signaling network 20 is shown. In order to avoid "on-line" exchange and agreement of security parameters, long-term security associations are established between signaling
20 points 30 and 32. In the PLMN networks 16 and 18 of the signaling network 20, the signaling points 30 and 32 know the key of every adjacent node equipped with a Security Functionality (SF) 22, independently of the type of node. Two nodes are adjacent, from the security point of view, if they have knowledge of their respective signaling point codes and can reach each other without the need
25 to involve an upper layer, such as the Signaling Connection and Control Part (SCCP), for Global Title (GT) re-translation. Internal signaling points know the keys of other internal signaling points and of at least one gateway signaling point of that network. Additionally, every gateway signaling point knows the keys of

the internal signaling points and of some gateway signaling points of the other networks.

The security parameters are linked to the signaling point address. This makes it possible for the type of security mechanism implemented inside one PLMN, such as mechanism 1 of Fig. 2, to be independent from the security mechanism implemented inside another PLMN, such as mechanism 3. Furthermore, the security mechanism adopted for the inter-PLMN leg, such as mechanism 2, is independent from the security mechanisms 1 and 3. This provides each operator with some flexibility in adopting the desired security solution.

In order to create a security association between two signaling points, each one having its own Secret Key (SK), the two signaling points might execute an appropriate protocol. The result is the choice of a security algorithm and the establishment of a SK, such as a key shared between the two nodes. Independent from how the two nodes identify each other and the type of key establishment protocol adopted, the result is a security association, such as an algorithm identifier and a key, known only to the two signaling points. This association can be used to secure the messages transferred between the two signaling points.

It is preferred that each signaling point have an SK stored securely, which cannot be accessed via software or hardware. The SK can be created by the signaling network administrator and manually stored in the node. Each signaling point can also have a table that contains all the security associations, such as identity of the other signaling, type of algorithm, and key to be used. The identity of the signaling point might be given by its signaling point code, and the security association can be created on the basis of the signaling point code.

Although different implementations are possible, for the sake of generality, a transparent SF introduced between the SCCP and the MTP3 protocol layers is considered in the embodiment shown in Fig. 2. The MTP3 signaling network functions correspond to the lower half of the OSI network layer and provide for the transfer of messages between signaling points. SF will provide SCCP with the same primitives that MTP3 provides and will use regular MTP3 services.

In order to apply security to the message to be transferred, SF 23 has to select the appropriate security association between the signaling point where it resides and the Signaling Point (SP), such as SP 30, at the message destination.

The SF 22 is involved when there are requests of service from an SCCP 24 protocol layer and delivery of data units from an MTP3 26 protocol layer.

When the SF 22 receives a request from the SCCP 24 to deliver a message, it checks the called party address in the SCCP 24 message to derive the destination point code towards which the message has to be forwarded and accesses a security associations table 34 using this point code. If an entry is found, then the SF 22 applies the SK and algorithm as indicated in the entry to the SCCP 24 payload, adds an additional field called Security Parameters Indicator (SPI) containing the node SPC and invokes the MTP3 26 services as the SCCP 22 has done with SF 22. The SPI is preferably not ciphered, in order to allow the destination SF 22 to use it to select the security association. Extra security can be added by adopting an additional public key mechanism and applying the public key of the receiver node to also cipher the SPI. This secured information, which includes the SPI, is then transferred to the next signaling point 30.

When the SF 22 receives a data unit from the MTP3 26, it checks the SPC in the SPI and accesses the security associations table 34. If an entry is found, the SF 22 applies security in order to obtain the original SCCP 24 payload and the SCCP message is delivered to the upper layer.

The solution can be implemented either in a transparent way or in an integrated way. In order to implement the SF 22 in a transparent way it is necessary that the signaling point allow a new board implementing the SF 22 between the SCCP 24 and MTP3 26 protocol layers. If this is not possible, then either the integrated solution is adopted or an external box is used. In the second option, each signaling point will be connected to a "security box" that implements two protocol stacks with the layers up to the MTP3 26 and, on top of them, the SF 22. On the side of the signaling point, the security box will have a "dummy" signaling point code, while on the network side the security box will have the original signaling point code of the signaling node, thus allowing the

security box to receive all the messages directed to the signaling point. The security box will implement security as described above and will be transparent to the signaling point, thus avoiding any modification in the existing signaling point.

Referring now to Fig. 4, duplicating part of the global title translation functionality, already performed at the SCCP 24 protocol layer in signaling nodes, in a centralized Global Title Security Server (GTSS) 40 and the usage of the GTSS 40 to retrieve the security parameters needed to secure MAP dialogues. The GTSS 40 includes an I/O unit 41 coupled to other network entities via multiple connection 49a and 49b. The I/O unit 41 is coupled to a processor 42 that processes the information and manages the GTSS 40 according a program stored in a memory 43.

The GTSS 40 can be a dedicated Signaling Point that acts as the centralised manager for Mobile Application Part (MAP) security in each PLMN. As such, the GTSS 40 implements the SS7 protocol stack up to the TCAP layer and the GTSS 40 specific functionality is implemented as a MAP user protocol level using TCAP services. In order to be addressable both from inside the PLMN and from other PLMNs, the GTSS 40 is assigned both SPC and an E.164 number, and the signaling routing tables have to be updated in order to be able to route messages towards the GTSS 40.

Referring now to Fig. 5, a MAP Security Functionality (MSF) 50 is the security functionality that is invoked when the MAP-user 52 in a MAP node needs to open a dialogue with another MAP node. The MSF 50 is present in each MAP node and is logically located between the MAP-user and a TCAP layer 54. This way the MAP-user 52 won't see any modification in the service due to the presence of MSF 50. Addressing of the MSF 50 by the GTSS 40, Fig. 4, can be done in the same way the MSF 50 addresses the GTSS 40, i.e. based on SPC and the use of a dedicated Sub-System Number (SSN), and indicating to the SCCP 24 to perform routing on the SSN.

Preferably, each PLMN 16 and 18 is equipped with one GTSS, and each GTSS would be connected to the GTSSs in the other PLMNs through SS7 signaling links.

When the MAP-user 52 opens a dialogue, the request is intercepted by the MSF 50 and put on hold. The MSF 50 can then analyse the MAP-user request in order to understand if security has to be applied; this depends on the type of security solution that has been implemented and on the type of entities
5 that are communicating, as described in the following section. When needed, the MSF 50 contacts the GTSS 40 in order to obtain the security parameters of the MAP node with which the dialogue has to be opened. The MSF 50 provides the GTSS 40 with the original global title contained in the opening of the MAP dialogue and protects this message exchange with the security parameters
10 previously distributed by the GTSS 40.

The MSF 50 can also be used to apply caching of security parameters and security to the data transferred through the TCAP dialogue.

The MSF 50 can reside over the TCAP 54 or could be built-in in the TCAP layer and uses the TCAP 50 in the MSF-GTSS interactions and in MAP
15 dialogues. In MSF-GTSS interactions, the MSF 50 opens a dialogue with the GTSS 40 using the TCAP services in the same way a MAP protocol instance would do with another MAP protocol instance. In MAP dialogues, MSF intercepts MAP-user messages and applies security algorithms to the data transferred through the TCAP services.

20 For security interactions, specific information elements for TCAP messages have to be defined in order to use TCAP services or if the TCAP messages and information elements are used as they are, then their interpretation in security-aware MAP nodes, such as the MSF 50, have to be defined.

25 In order to implement partial security solutions or different levels of security for different types of MAP entities, it is possible to use the SSN as a discriminator or the TCAP field in the Security Context Identifier to indicate if the MAP message is protected or not.

30 As an example, if different security algorithms for different interfaces are desired, the MSF can examine the SSN included in the Calling Party addresses indicated in the opening request. If the two SSNs indicate that the dialogue is

between a VLR and a HLR, or vice versa then security is applied, otherwise MSF doesn't take any action.

Referring now to Fig. 6, a signaling function 60 is shown. The signaling function 60 includes an I/O unit 61 coupled to other network entities via multiple connection 69a and 69b. The I/O unit 61 is connected to a microprocessor 62 for processing the information and managing the signaling function 60 according to instructions stored in a memory 63. The security function 60 comprises an I/O unit 61 connecting it to other network entities possible via multiple connection 69a, 69b. The I/O unit 61 is connected to a microprocessor 62, processing the information and managing the signaling function 60 according a program stored in a memory 63

Referring now to Fig. 7, a PLMN 70 using a GTSS, such as GTSS 40, in establishment of intra-PLMN connections is shown. The visitor location register (VLR) 72 opens a dialogue when a MAP user request is intercepted by the MAP security functionality in a MAP node 74 and translated into a query 72 towards the GTSS 40. The GTSS 40 will attempt to translate the global title in order to understand if it is related to an entity inside the PLMN 70 or if it belongs to another PLMN. In the first case, the GTSS 40 returns 73a the security parameters needed in order to secure the dialogue as the translation of the global title. The GTSS 40 also contacts the destination entity A2 indicated by the global translation and provides 73b the security parameters of the Map Node 74 initiating the dialogue. Using said security parameters a secure signaling connection 76 is established between the Map Node 74 and a Map Node 78 at the destination entity A2.

Referring now to Fig. 8, a case where the MAP entity B1 indicated by the global title belongs to PLMN B, then a GTSS 86 has to be contacted. The GTSS 76 sends a query 81 to the GTSS 86 in the PLMN B network. The GTSS 86 will translate the global title provided by the GTSS 76 and return a security parameter 82 to the GTSS 76. The GTSS 86 also delivers the security parameter of a Map Node 84 initiating the dialogue to a destination Map Node 88 indicated by the GT translation. The GTSS 76 returns the global title translation and the security parameters received to the Map Node 84 where the dialogue is

initiating. At this point, after security is applied to the payload contained in the message of the MAP dialogue, the MSF invokes TCAP services to proceed with the dialogue and a secure connection between MAP Nodes 84 and 88 is established at path 74.

5 In a more detailed way, addressing of GTSS by the MSF can be based on signaling point code because each MSF knows the signaling point code of the GTSS and use of a special SSN and indicating to SCCP to perform routing on SSN. Addressing between GTSSs, the query 81, can again be based on signaling point codes and the dedicated SSN. Either the value 00001010 or
10 11111111, already reserved in MAP and Q.713 respectively for the Authentication Centre and for expansion of national and international SSN, can be used as SSN for the GTSS.

 The GTSS implements security management for the management and retrieval of security parameters, global title interpretation, and caching of security
15 parameters.

 The GTSS would be used for inter-PLMN signaling except when, as shown in the follow, a caching functionality is present in every node and contains useful data.

 From the security point of view, the GTSS would act as a security server
20 for the PLMN and would manage the following levels of security parameters:

1. create, distribute, and manage the security parameters that will be used to secure the MAP dialogues between MAP entities, both for inter-PLMN and for intra-PLMN cases;
2. optionally, it would create, distribute, and manage the security
25 parameters needed to create a security association between each MAP entity in the PLMN and the GTSS. These security associations are used to protect the signaling messages exchanged between any MAP entity and the GTSS when intra-PLMN security is implemented; and
3. optionally, it would store and co-operatively update the security
30 parameters used to secure dialogues with other GTSSs.

Both public key methods and private key methods can be used to secure the different dialogues. When public key algorithms are used for inter-PLMN dialogues, the GTSS would act as a certificate authority for all the nodes in the PLMN, distributing and certifying public keys. In case public key algorithms are used also for intra-PLMN MAP dialogues and/or for MSF-GTSS dialogues, the GTSS would act again as a certificate authority for all the nodes in the PLMN. If private key algorithms are used instead, the GTSS will generate and distribute the secret keys to be used to secure intra-PLMN dialogues and/or MSF-GTSS dialogues.

Depending on the implementation, the keys and the algorithms used for inter-PLMN and for intra-PLMN dialogues could be the same, and they could also correspond to the ones used for dialogues between the MAP entities and the GTSS. Different levels of security can be implemented for the intra-PLMN and the inter-PLMN cases, but also for different types of MAP entities, such as different keys and algorithms applied on the basis of the SSN used.

If the global title interpretation is implemented in the GTSS then it would incorporate a subset of the SCCP GT translation capability in order to be able to "interpret" a global title. In particular, the GTSS has to be able to derive from the global title the identity of the PLMN to which the global title is referring.

When the GTSS is contacted by the MSF in order to translate a global title and retrieve the associated security parameters, the GTSS derives the identity of the target PLMN from the global title using the Country Code and Network Code contained in it.

If the global title refers to the same PLMN in which the GTSS is located, the GTSS would simply use the remaining part of the global title to access the table where the parameters associated to the target entity are stored, since those parameters have been previously allocated by the GTSS itself.

In the case that the global title refers to another PLMN, the GTSS would contact the appropriate GTSS requesting the parameters associated with the target global title.

To optimise the solution a caching function can be introduced to reduce the need for using the GTSS to reach the target PLMN and obtain the security parameters of the target entity and achieve a better usage of the signaling links. The caching function stores the security parameters associated to a MAP entity
5 addressed by a GT, in order to retrieve them immediately when a dialogue towards the same MAP entity has to be opened using again the same GT.

Three different levels of caching are foreseen:

1. one cache level: when only one cache level would be available, the cache functionality can be either in the GTSS or in the MAP nodes. If the
10 cache is in the GTSS, the MSFs have always to contact the GTSS even if the same GT is addressed frequently by a single node. Anyway, when more than one GTSS is present in one PLMN and the cache is only in the GTSS, the management of the cache content could become difficult if the same level of cache effectiveness provided when only one GTSS is
15 present has to be maintained. On the contrary, if the cache is in MAP nodes, when a MAP node uses a GT for which his cache doesn't have any entry, it is necessary to reach the other PLMN GTSS although the entry might be present in the cache of another MAP node;

2. distributed (two levels) cache: the cache functionality would be
20 present both in the GTSS and in MAP nodes. A possible way of managing two levels of cache in order to minimise the need of reaching another GTSS while maintaining the cache size as small as possible is to associate each entry with different timestamps in the two caches, with timestamps in GTSS greater than in MAP nodes; and

3. semi-distributed (two levels) cache: the cache functionality would
25 be present in the GTSS and in "popular" MAP nodes, where popular indicates those nodes where the probability of using a GT towards another PLMN is maximised, such as VLR in popular areas such as airports, where a large number of roaming users register.

30 In the distributed cases the content of the cache could be semi-permanent, which is based only on the parameters lifetime specified by the

PLMN that has generated them, if global parameters are allocated. When caching is used, the MSF acts as described above but, before contacting the GTSS, it would check if any entry is available in the cache for the destination MAP entity. If not, then the MSF would contact the GTSS as described above,
5 otherwise applies the security parameters retrieved from the cache.

Each entry of the cache can have a limited temporal validity. This is done to allow both to refresh obsolete security parameters and to keep the cache occupancy under control. Each cache entry is associated with two time-stamps:

1. A first time-stamp would indicate the maximum temporal validity of
10 the security parameters, as designated by the originating PLMN (the value is transferred from the originating PLMN together with the security parameters); and
2. A second time-stamp indicates the maximum temporal validity of
15 the entry, as designated by the operator-specific cache management policy when the entry has been created.

To build an inter-PLMN security infrastructure, as already indicated above, GTSSs share security associations among themselves. The scope of these security associations is to allow entity authentication and the establishment of a secure communication channel.

20 Each GTSS would maintain a table where, for each GTSS it shares a security association with an entry containing the Country Code of the PLMN and the Network Code of the PLMN, the GTSS address (an E.164 number) and the security keys is stored.

25 These security associations could be either semi-permanent, i.e. manually defined by network administrators at the roaming agreement time, such as a hot-start, or updated dynamically through an off-line protocol, based on a hot-start. Since the security associations among GTSSs can be updated off-line, they won't create any concern from the point of view of signaling performances.

30 For inter-GTSS relations, public key methods can be used and a certification authority has to be chosen to validate the public keys. The

determination of an authority or multiple authorities suitable to act as a certification authority(s) would be based not only on technical issues, such as location and time required for the verification, but also on political agreements between operators.

5 Private key methods can be used to secure inter-GTSS communications if a certification authority cannot be chosen. In this case, the system has to be bootstrapped by manually storing in the GTSSs the keys agreed between pairs of operators.

10 Although in principle an operator could choose not to have security for intra-PLMN signaling, the proposed solution is based on the security of this relation. A secured MSF-GTSS relation allows creating and distributing the keys needed for MSF to MSF communications in a safe way.

15 The GTSS would maintain a table where, for each MAP entity in the PLMN, the current security keys are stored. Each entry will contain both the keys used for the inter-PLMN case and for MSF-GTSS dialogues. The GTSS is also in charge of periodically updating these keys.

20 Security for intra-PLMN MAP dialogues is strongly recommended to implement intra-PLMN MAP security. Moreover, although in principle it is possible to have different inter-MSF security mechanisms for the intra-PLMN and the inter-PLMN cases, it is strongly recommended to implement just one mechanism for both cases.

25 Entity authentication has to take place only between GTSS. For MSF to MSF interactions, authentication of data origin and encryption integrity are considered, because MSF-GTSS and GTSS-GTSS relations are seen as trusted. Accordingly, MSF to MSF communications can be based on the use of both independent sets of parameters and individual parameters. As in the case of MSF to GTSS, two session keys would be used and applied, respectively, to a cryptographic checksum and a stream cipher to provide integrity and confidentiality.

30 The additional fields that can be added to each message that would be the cryptographic checksum and be ciphered together with the MAP message

payload with a security header indicating the type of security applied if multiple alternatives are available. Ciphering will be applied to the entire MAP message except the security header, the Calling Party address, and the Called Party Address.

5 When individual sets of parameters are used, the establishment of session keys to be used between two MSFs can take place in two possible ways:

internally to the GTSS to which both MSFs belong (intra-PLMN case); and

between the two GTSSs to which the MSFs respectively belong, such as in inter-PLMN case and intra-PLMN case when multiple GTSSs are
10 present in a PLMN.

If independent sets of global parameters will be used instead, it would be not necessary to establish a pair of keys for each pair of MSFs in the network, but only a pair of keys for each type of entity (e.g. VLR and HLR). In this case, within each PLMN the GTSS will create the pairs of keys needed to secure
15 communications within that PLMN.

These keys will again be associated with a temporal validity, but in this case the GTSS will initiate the key updating using either a MAP version or a security negotiation. A security negotiation, on the other hand, is a type of negotiation necessary for compatibility with networks where security has not
20 been introduced and to allow the introduction of security step-by-step. In one situation the GTSS does not have any entry for a target GTSS in the target PLMN, indicating that security is not present in the target PLMN or that an agreement has not been established yet, then the MSF behaves transparently. In another situation, the GTSS will receive an indication from the target GTSS if
25 security has to be applied for the target node. Depending on the implementation choices, if security is integrated inside the MAP protocol the two negotiations can take place at the same time.

A MAP version is the normal negotiation that takes place in MAP dialogues. In a transparent implementation, the MSF would be implemented as
30 a new protocol layer offering to MAP the same SAPs offered by TCAP and using TCAP services. This solution assumes that the MSF can be installed as a new

software module or as a hardware board on MAP nodes between the MAP and the TCAP protocol layers. When the MSF puts the MAP dialogue on hold in order to contact the GTSS, then the total time needed for establishing the dialogue with the GTSS, contacting the target GTSS, and obtaining the security
5 parameters has to be less than the maximum time allowed by the MAP protocol to receive an answer for a sent MAP message, which is called protocol time-out

In an integrated implementation, the MSF would be integrated in the MAP protocol. This solution allows the optimisation of the protocol, because all possible problems related to protocol timers due to the application of security and
10 the use of TCAP services to transport security messages will be directly solved inside the MAP protocol. MAP messages are modified in order to add the fields needed for the security mechanism.

Accordingly, it is possible to achieve secure signaling connection between two network entities in a telecommunication network. This secure connection
15 can be achieved with a security functionality that is independent of the layer of protocol stack over.

The process of establishing a secured signaling connection between two network entities in order to transmit and receive secured information begins at step 100. At step 110, a first network entity obtains the security parameters of a
20 second network. At step 120, the security parameter is used to transform the information into a secured information. At step 130, the secured information is transmitted from the first network entity to the second network entity. At step 140, the second network entity recovers the information from the secured information and the process ends at step 150. Additionally, the second network
25 entity can obtain the security parameters of the first network entity and if the security parameter of the first network entity is used to secure information, then the second network entity can use that to recover information from the secured information transmitted from the first network entity to the second network entity. Furthermore, the second network entity can use the security parameters of the
30 first to secure information transmitted from the second network entity to the first network entity.

It will be apparent to those skilled in the art that the teaching set forth herein is not limited by the type of entities between which the signaling information is exchanged. For example, the entity could be any kind of digital switch present in a telecommunication network, like a mobile switching centre (MSSC), a visitor location register (VLR), a home location register (HLR), a or
5 base station controller (BSC).

It is evident to a person skilled in the art that various modifications may be made within the scope of the invention. In particular it is recognised that the security functionality can be located also in other parts of the protocol stack other
10 than the ones described, as long as the security functionality has access to signaling point addresses.

Although described in the context of particular embodiments, it will be apparent to those skilled in the art that a number of modifications to these teachings may occur. Thus, while the invention has been particularly shown and described with respect to one or more preferred embodiments thereof, it will be
15 understood by those skilled in the art that certain modifications or changes, in form and shape, may be made therein without departing from the scope and spirit of the invention as set forth above and claimed hereafter.

What is claimed is:

1 1. A method for securing signaling connection within
2 communication networks, the networks including a first network entity having
3 signaling information to be sent to a second network entity and the first
4 network entity having access to a security parameter of the second network
5 entity, the method comprising:

6 obtaining the security parameter of the second network entity from the
7 first network entity;

8 using the security parameter to transform the signaling information into
9 a secured signaling information;

10 sending the secured signaling information from the first network entity
11 to the second network entity; and

12 recovering the signaling information from the secured signaling
13 information.

1 2. The method of claim 1 wherein the security parameter is located
2 in a protocol stack.

1

1 3. The method of claim 1 wherein the security parameter is
2 associated with at least to signaling addresses of the network entities.

1

1 4. The method of claim 1 further comprising accessing a security
2 parameter of the first network entity from the second network entity and using
3 the security parameters of the first network entity to transform signaling
4 information.

1

1 5. The method of claim 1 wherein the security parameter is used to
2 cipher the signaling information.

1

1 6. The method of claim 1, further comprising authenticating the
2 first network entity to the second network entity using the security parameter.

1

1 7. The method of claim 1 further comprising sending the signaling
2 information using Internet Protocol.

1

1 8. The method of claim 1 wherein the first network entity has at
2 least one security parameter reserved for connection with a third network
3 entity.

1

1 9. The method of claim 1 further comprising exchanging
2 information about the security parameter between the first network entity and
3 the second network entity via a third network entity.

1

1 10. The method of claim 1 further comprising requesting by the first
2 network entity the security parameters of the second network entity from a
3 third network entity.

1

1 11. The method of claim 10 wherein the security parameter of the
2 second network entity is stored in a fourth network entity and the third
3 network element requests the security parameter of the second network entity
4 from the fourth network entity.

1 12. The method of claim 11 wherein the third and fourth network
2 entity are located in different networks.

1

1 13. The method of claim 1 wherein the second network entity is a
2 first gateway connecting one network to a second gateway of another
3 network.

1

1 14. The method of claim 13 wherein the first gateway has access to
2 the security parameter of the second gateway and the second gateway has
3 access to the security parameter of the first gateway and the first and second
4 gateway use the security parameters to secure the signaling connection
5 between the first and second gateway.

1

1 15. A network element in a telecommunication network comprising:
2 means for sending and receiving information;
3 means for accessing a security parameter of at least one
4 network entity; and
5 means for establishing a secure signaling connection according
6 to the security parameter to the at least one network entity.

1

1 16. The network element of claim 15 further comprising means for
2 storing the security parameter of the at least one network entity.

1

1 17. The network element of claim 15 further comprising means for
2 accessing the security parameter of the second network entity from a third
3 network entity.

1

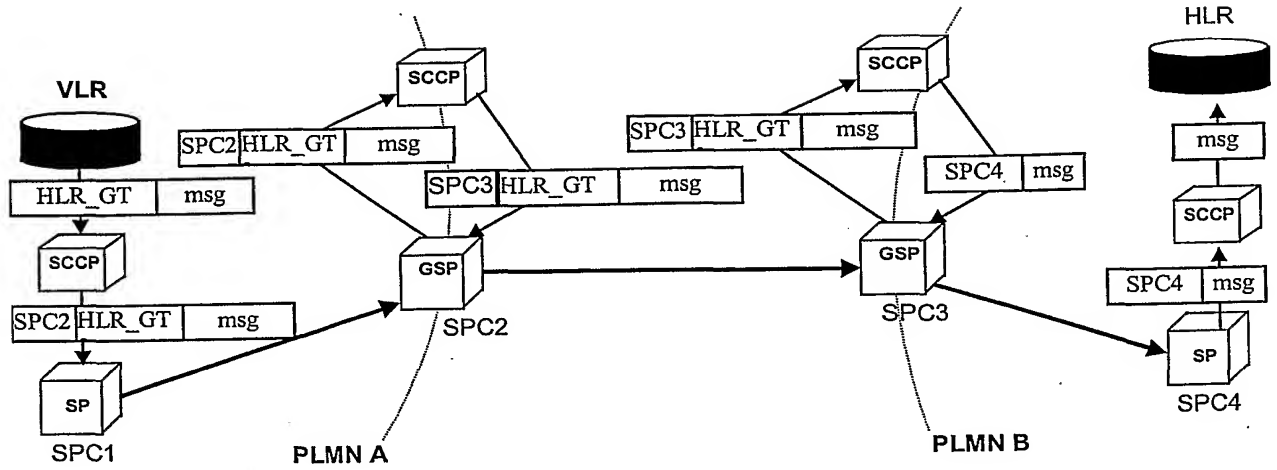
1 18. The network element of claim 17 further comprising means for
2 caching the received security parameters.

1

1 19. A telecommunication network comprising:
2 a first network element having means for sending and
3 receiving signaling information;
4 means for accessing security parameters of a second
5 network element; and
6 means for establishing a secure signaling connection
7 between the first and second network element according the
8 security parameters.

1
1 20. The telecommunication network of claim 19 wherein the first
2 network element comprises means for storing the security parameters of the
3 second network entity.

1
1 21. The telecommunications network of claim 19 further
2 compromising:
3 a third network element having means for receiving inquiries
4 from the first network element about the signaling security
5 parameters of the second network element;
6 means for accessing the signaling security parameters; and
7 means for sending the signaling parameters to the first network
8 entity.



Prior Art
Fig. 1.

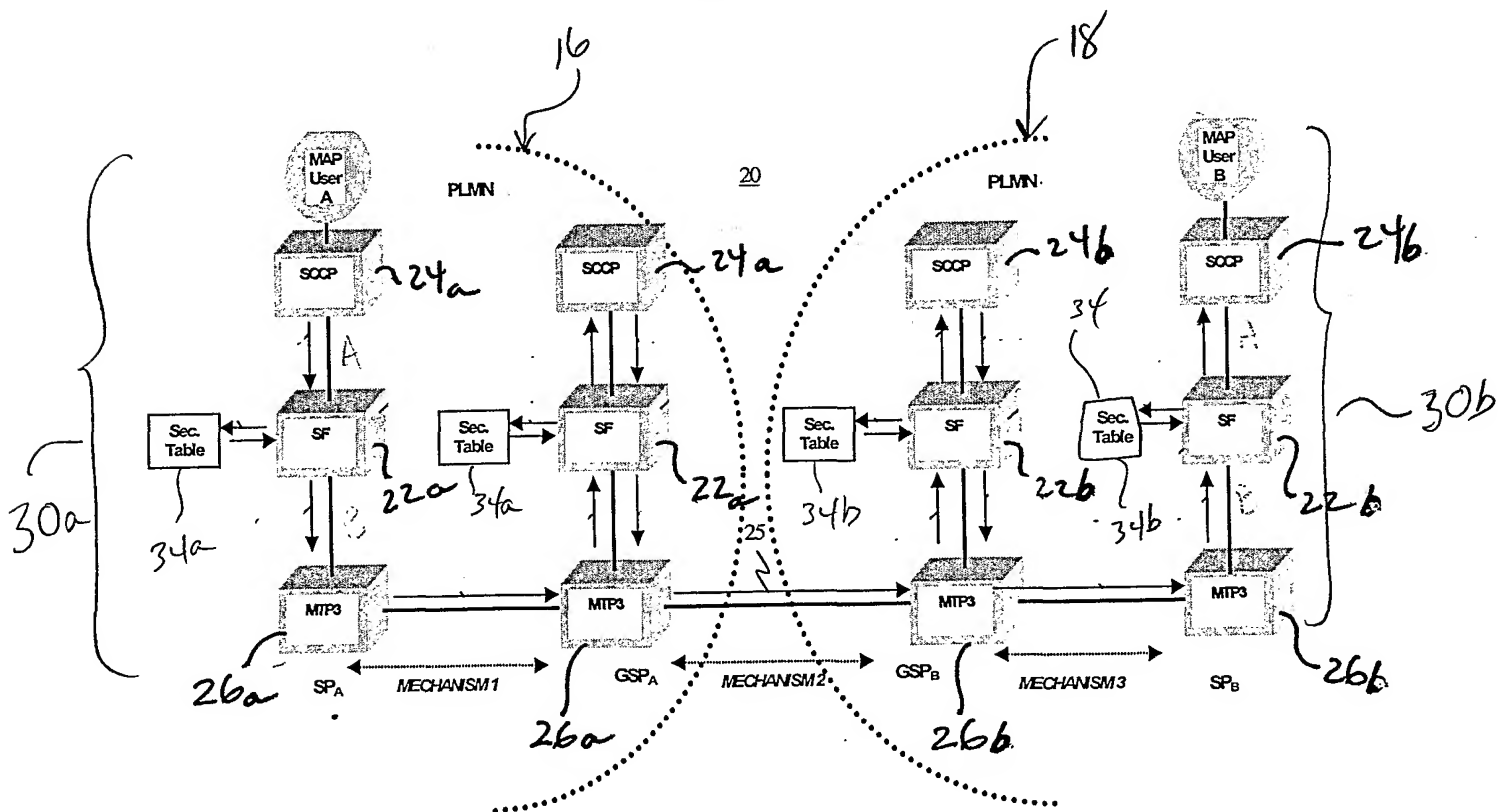


Fig. 2.

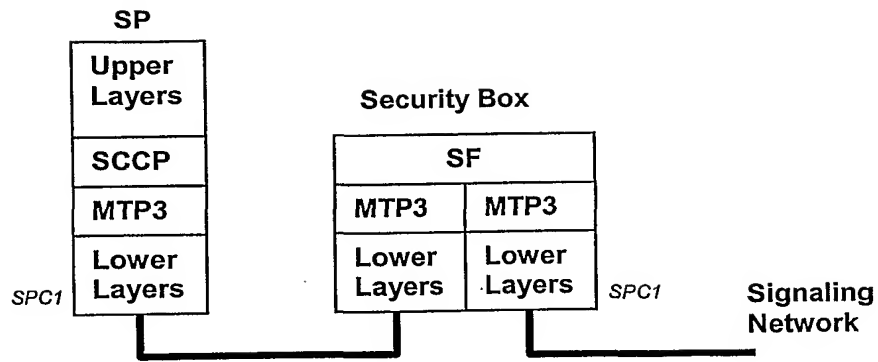


Fig. 3

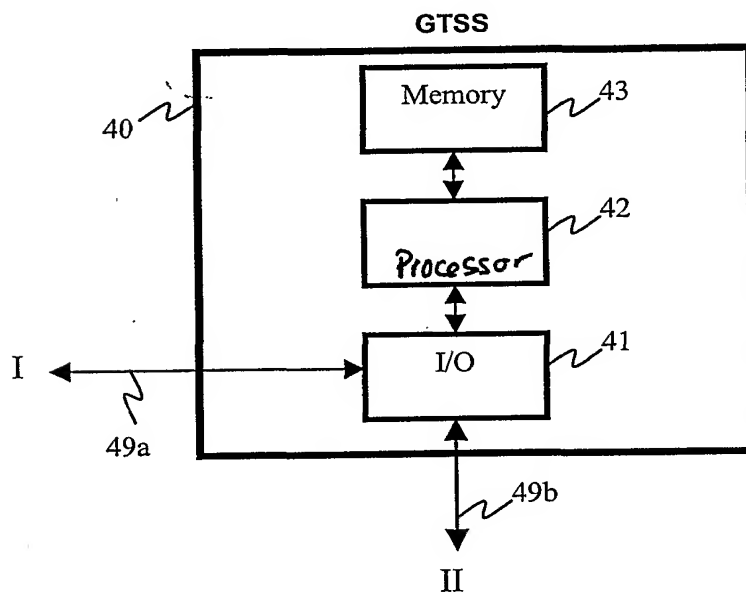


Fig. 4

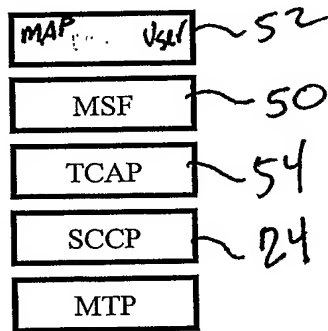


Fig. 5

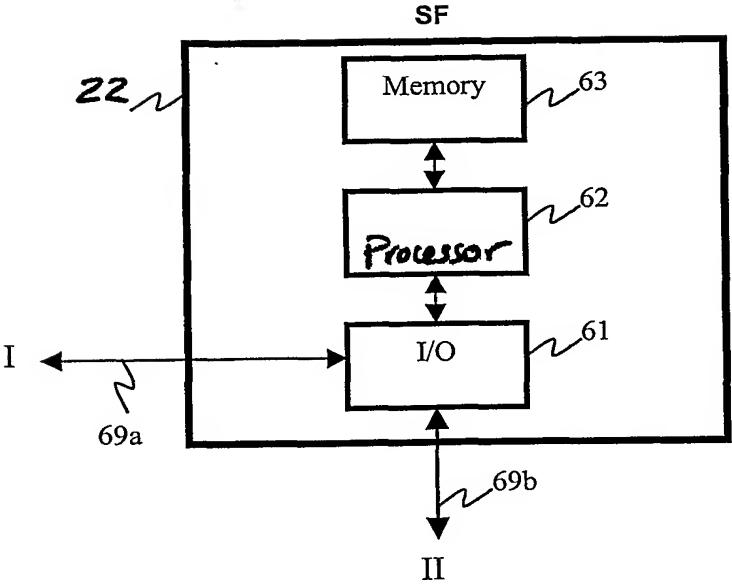


Fig. 6

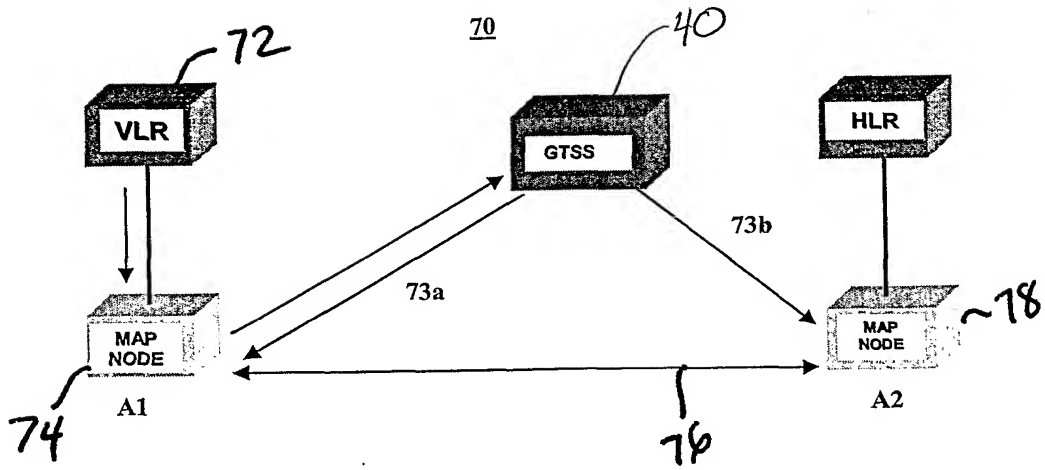


Fig. 7

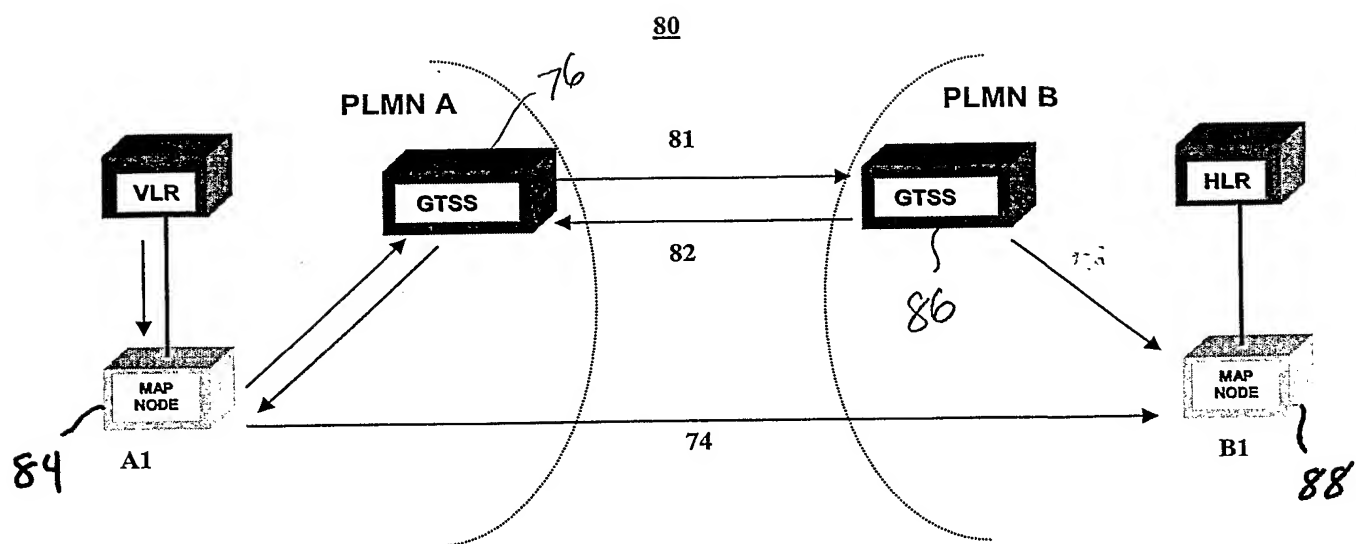


Fig. 8

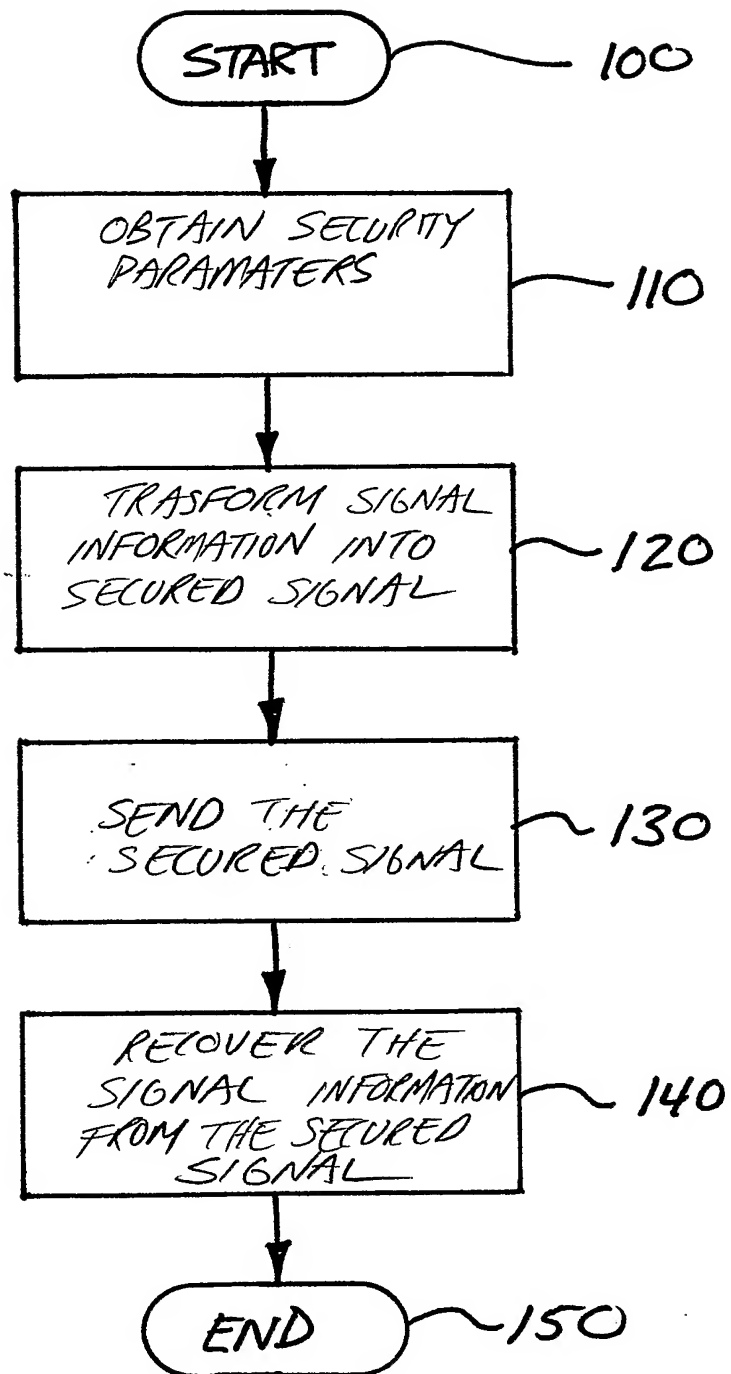


Fig. 9

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
7 February 2002 (07.02.2002)

PCT

(10) International Publication Number
WO 02/011395 A3

- (51) International Patent Classification⁷: **H04L 29/06**
- (21) International Application Number: PCT/US01/24153
- (22) International Filing Date: 31 July 2001 (31.07.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
09/630,031 31 July 2000 (31.07.2000) US
- (71) Applicant (for all designated States except US): **NOKIA NETWORKS OY** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): **FACCIN, Stefano** [IT/US]; 3421 Dartmoore Drive, Dallas, TX 75229 (US).
- (74) Agents: **RIVERS, Brian, T.** et al.; Nokia Inc., 6000 Connection Drive, MS 1-4-755, Irving, TX 75039 (US).

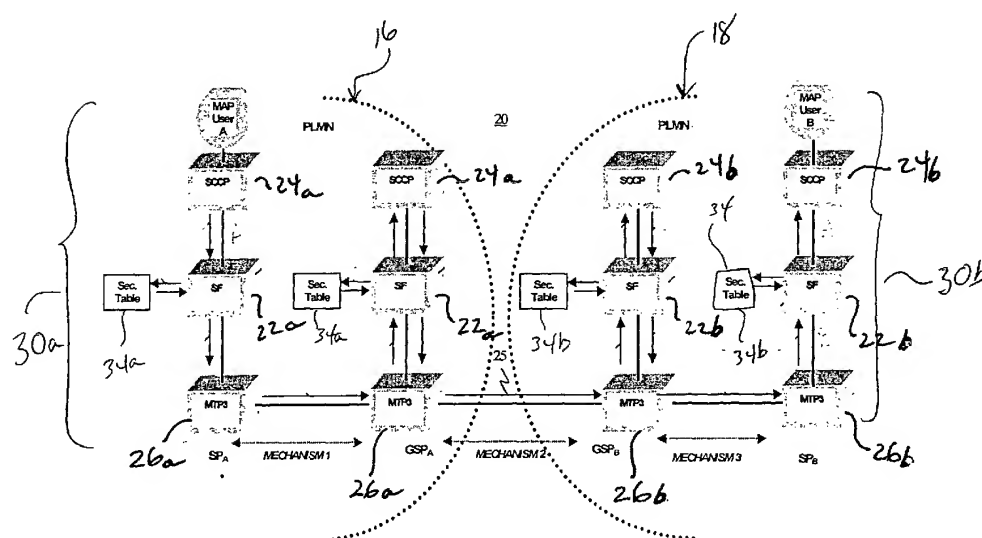
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

[Continued on next page]

(54) Title: METHOD FOR SECURING INFORMATION EXCHANGES IN A TELECOMMUNICATION NETWORK



(57) Abstract: A system (Fig. 2) and a method are provided for securing signaling connections in telecommunication networks and to provide network functionalities (22a, 22b) to secure the signaling connection between network elements. The security parameters (34) are associated with the addressing of signaling information preferably using global titles (GT) or signaling point codes (SPC). The method for securing signaling connection within communication networks includes the steps of obtaining a security parameter (34) of a second network, using the security parameter (34) to transform the signaling information into a secured signaling information, sending the secured signaling information to the second network entity (26b), and recovering the signaling information from the secured signaling information.



(88) Date of publication of the international search report:
19 September 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 01/24153

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, X	<p>WO 01 08377 A (NORTEL NETWORKS CORP ;RAO SANJAY H (US); OXENDINE KENNETH W (US)) 1 February 2001 (2001-02-01) abstract page 1, line 12 - line 29 page 2, line 15 -page 3, line 16 --- -/--</p>	1-21

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search

15 July 2002

Date of mailing of the international search report

22/07/2002

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Adkhis, F

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 01/24153

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	<p>SCHULZRINNE H ET AL: "Internet Telephony: architecture and protocols - an IETF perspective" COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, vol. 31, no. 3, 11 February 1999 (1999-02-11), pages 237-255, XP004304601 ISSN: 1389-1286 abstract page 238, left-hand column, line 23 -right-hand column, line 16 page 240, right-hand column, line 33 - line 38 page 246, left-hand column, line 23 -page 247, left-hand column, line 25 -----</p>	1,15,19

INTERNATIONAL SEARCH REPORT
information on patent family members

International Application No
PCT/US 01/24153

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
WO 0108377	A	01-02-2001	AU	6223300 A		13-02-2001
			EP	1145521 A2		17-10-2001
			WO	0108377 A2		01-02-2001
<hr/>						